

ACAS Operational Attribute Tagging Using COAMS and CMRS

March 8, 2018

V4

Table of Contents

[Change Log 2](#_Toc508610406)

[Introduction 3](#_Toc508610407)

[Standards and Conventions 3](#_Toc508610408)

[Abbreviations 4](#_Toc508610409)

[Asset tagging 4](#_Toc508610410)

[COAMS Viewer Background information 4](#_Toc508610411)

[Getting COAMS Data 4](#_Toc508610412)

[Updating COAMS Viewer Catalogs 5](#_Toc508610413)

[COAMS Viewer User Interface 5](#_Toc508610414)

[Using COAMS Viewer in SecurityCenter 6](#_Toc508610415)

[Using CMRS in SecurityCenter 14](#_Toc508610416)

[Common Errors 19](#_Toc508610417)

[Superseding Error 20](#_Toc508610418)

[Invalid Timestamp Error 20](#_Toc508610419)

[Data Type Identifier Error 20](#_Toc508610420)

[Timestamp Missing Error 20](#_Toc508610421)

[Partial Update Error 21](#_Toc508610422)

[Partial Update Value Error 21](#_Toc508610423)

[Missing Parent Error 21](#_Toc508610424)

[Publishing Error 22](#_Toc508610425)

[Useful links 23](#_Toc508610426)

# Change Log

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Changes** |
| 8-March-2018 | 4 | * Added SecurityCenter (SC) 5.6.x screen captures. * Edited content to reflect new SC navigational changes. * Added additional navigation instructions to several sections as needed. * Update “Useful Links” section. |
| 27-August-2015 | 3 | * Adding the following caveat on page 5: CMRS will not accept the following characters when publishing from SecurityCenter: “&”, “>”, or “<”. * Replaced the screenshot in Step 2 on page 7. * Revised the paragraph below the new screenshot on page 7. * Replaced the screenshot in Step 3 on page 8. * Added the following caveat on page 12: The values “true” or “false” must be in all lowercase. * Moved the “COMMON ERRORS” section * Added the “PUBLISHING ERROR” subsection under “Common Errors” section. * Change Log and Useful Links sections added. |
| 13-Feb-2015 | 2 | * Updated content to reflect information for COAMS Viewer version 1.2. |
| 19-Dec-2013 | 1 | * Initial document creation. |

# Introduction

This document describes the use of Cyber Operational Attributes Management System (COAMS) Viewer to interface with the Tenable Network Security SecurityCenter for publishing data into Continuous Monitoring Risk Scoring (CMRS). A new feature was added to SecurityCenter to support publishing results for a vulnerability scan. This new feature allows users to publish reports from SecurityCenter to a third-party system. Users can configure the reports to be published automatically or manually pushed. The reports generated will be in an Asset Reporting Format (ARF) and Asset Summary Reporting (ASR) format. The output file can be published to CMRS. This system requires the use of WS-Notification and the CMRS publishing is designed to work for that system. Another option is to publish to a Hypertext Transfer Protocol (HTTP) site, which uses a simple HTTP POST method and uses BASIC Auth. This allows the user to publish to an external system.

COAMS Viewer is an external Defense Information Systems Agency (DISA) tool which will be used for inserting the proper naming structure for assets. COAMS is a repository of authoritative sources for names where new names can be created if there is a gap or where classification or sensitivity issues make re-using existing repositories impossible. Embedded in this document are the instructions on how to setup and manage that tool called the COAMS Viewer.

## Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the UNIX **pwd** command:

# **pwd**

/opt/sc4/daemons

#

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Important notes and considerations are highlighted with this symbol and grey text boxes. |

|  |  |
| --- | --- |
| LoRes_Lightbulb2.png | Tips, examples, and best practices are highlighted with this symbol and white on blue text. |

## Abbreviations

The following abbreviations are used throughout this documentation:

CMRS Continuous Monitoring and Risk Scoring

SC SecurityCenter

COAMS Cyber Operational Attributes Management System

ACAS Assured Compliance Assessment Solution

ARF Asset Reporting Format

ASR Asset Summary Reporting

XML Extensible Markup Language

# Asset tagging

Before a SecurityCenter user can use the publishing services to an external system such as CMRS, the user must understand the logic behind the publishing of data. The goal is to simplify the asset tracking and security information. The ACAS solution has the capability to publish security scan results to an external system as long as it can understand the DoD approach to tagging and asset using an Extensible Markup Language (XML) format. The ACAS system can build the XML in two DoD formats: Asset Summary Reporting (ASR) and Asset Reporting Format (ARF). The primary goal of the ASR format is to describe summary information about one or more DoD assets in a standardized manner and ASR can be used as a payload for an ARF output. ACAS is considered an ASR reporter where CMRS is considered and ASR consumer. In order to publish the asset data, ACAS uses an external tool called COAMS Viewer to standardize the DoD naming structure of the assets. The combination of COAMS and ACAS provides usable asset tagged data to CMRS.

# COAMS Viewer Background information

The goal for COAMS is to simplify and standardize the naming structure for DoD. COAMS will be used at the Cyber Command level to ensure proper naming. The COAMS Viewer allows users to update COAMS catalog files to use the most recent and up-to-date data. COAMS Viewer can be downloaded from:

<https://software.forge.mil/sf/frs/do/downloadFile/projects.cm_vm/frs.coams_viewer_1_2.coams_viewer_1_2_fully_release_p/frs11427?dl=1>

## Getting COAMS Data

To get the latest COAMS data follow the instructions below.

1. **Login** into COAMS website at <https://dpms.disa.mil/coams/home>.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Access to the Digital Policy Management System (DPMS) requires completion and approval of a System Authorization Access Request (SAAR), Form 2875. |

1. **Click** the Export tab.
2. **Select** the COAMS Data Type in the Name Type box. (e.g. Organization, Location, and System)
3. **Click** Omit Date.
4. **Click** Export.
5. **Save** the file.
6. Repeat **Steps** **2** through **6** until the **Organization**, **Location**, and **System** fields have all been exported.

## Updating COAMS Viewer Catalogs

The COAMS Viewer comes pre-packaged with Organization and Location COAMS catalog files. To update the COAMS Viewer with the latest COAMS catalog files, follow the instructions below.

1. **Close** the COAMS Viewer.
2. **Copy** the latest COAMS catalogs into the COAMS Viewer directory.
3. **Start** COAMS Viewer by executing CoamsViewer.exe.

The COAMS Viewer loads data from the latest COAMS catalog file of each Data Type. (e.g. Organization and Location) available in the Viewer directory.

# COAMS Viewer User Interface

The COAMS Viewer UI allows users to select the COAMS Data Type, Rollup and traverse the hierarchical tree to copy the Fully Qualified Name of the selected tree element.

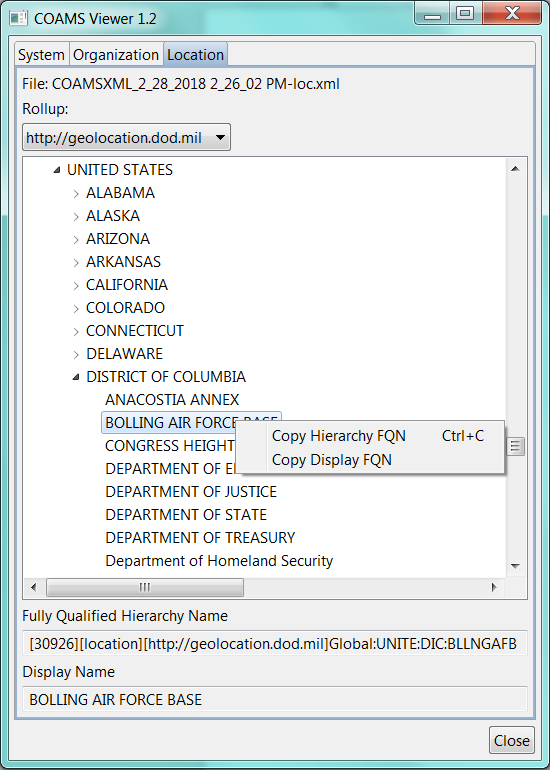


Figure 1 - COAMS Viewer UI

### 

* **Tabs** represent the COAMS data types (e.g. System, Organization, Location) of the COAMS catalog files loaded from the Viewer directory.
* **File** shows the name of the loaded COAMS file.
* **Rollup** select box displays the rollup views available for the current COAMS Data Type. A rollup is an alternative view of the same data set tailored for a specific purpose. The default rollup is the first item in the rollup select box.
* The **Tree View** displays the data from the currently selected **COAMS Data Type** and **Rollup**. Selecting an element populates the **Fully Qualified Hierarchy Name** and **Display Name** text boxes. Right clicking on the element gives the option to copy either field to the clipboard.
* **Fully Qualified Hierarchy Name** displays the unique COAMS ID in brackets and the Fully Qualified Hierarchy Name.
* **Display Name** displays the readable name for the selected element.

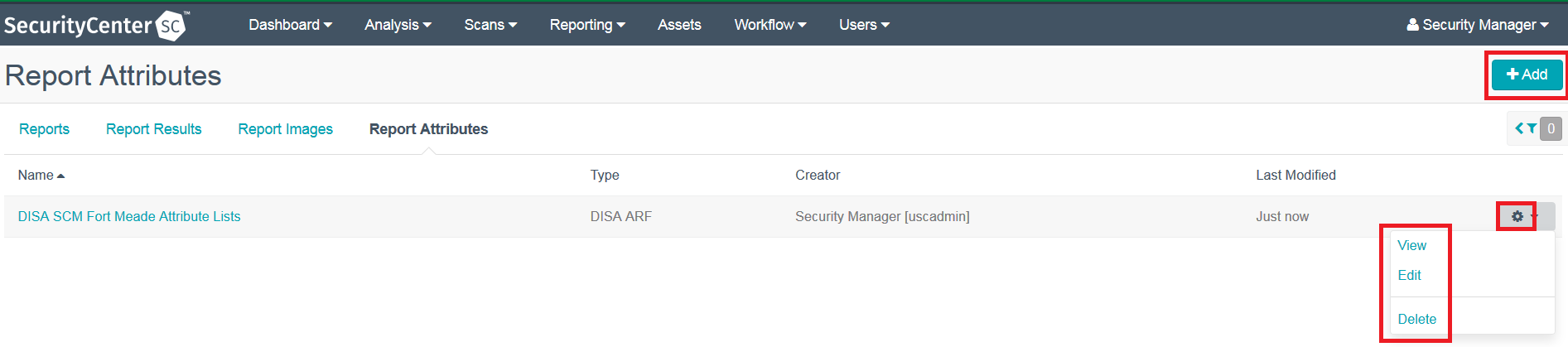
# Using COAMS Viewer in SecurityCenter

Once the COAMS Viewer has been installed on a Windows workstation, the user will be able to use the interface to select an origination in DoD for asset naming.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | CMRS will not accept the following characters when publishing from SecurityCenter: “&”, “>”, or “<”. Ensure that these three characters are removed when copying and pasting COAMs information into the operational attributes in SecurityCenter. See the “Publishing Error” section under “Common Errors” of this document for more details. |

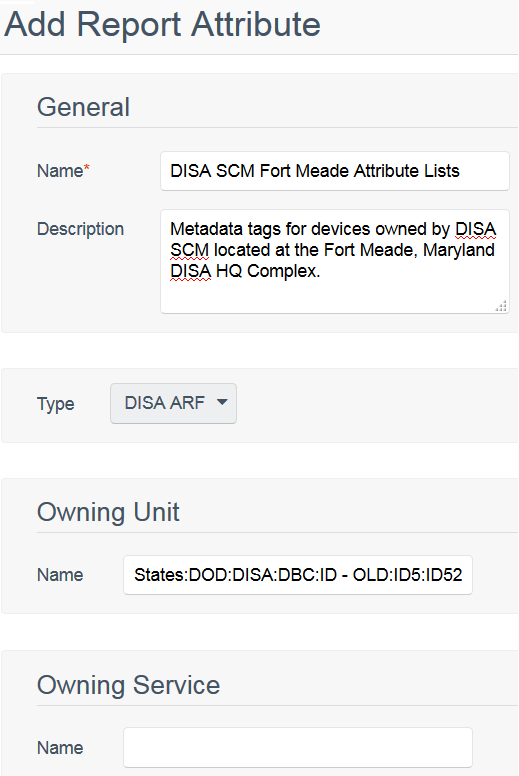
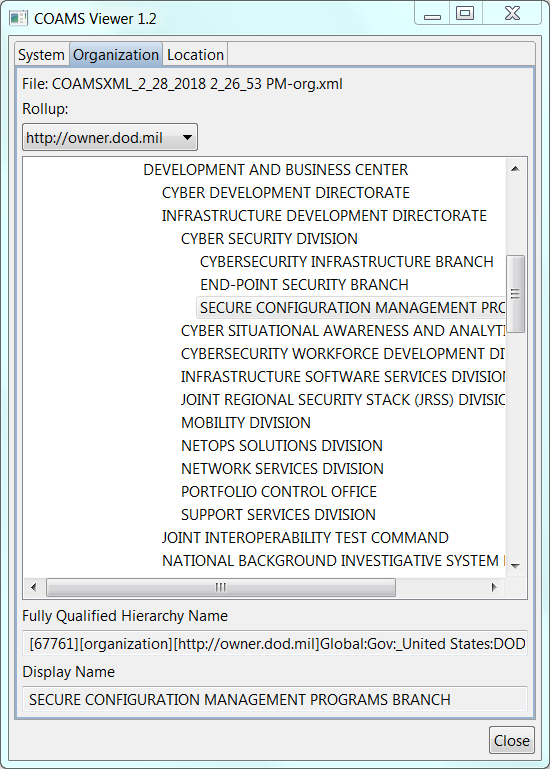
|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | In each of the following steps, the COAMS Viewer is on the left dialog box and the right is the location in the ACAS SecurityCenter. |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | The SecurityCenter needs to be logged into by a Security Manager user account and the Attribute rights needs to be opened in order to fill out the appropriate Attribute Set. |



To create a new Report Attribute in SecurityCenter, log in as an Organization user and click “Reporting” then “Report Attributes”. To add a new Report Attribute click the “Add” button.

***Step 1***



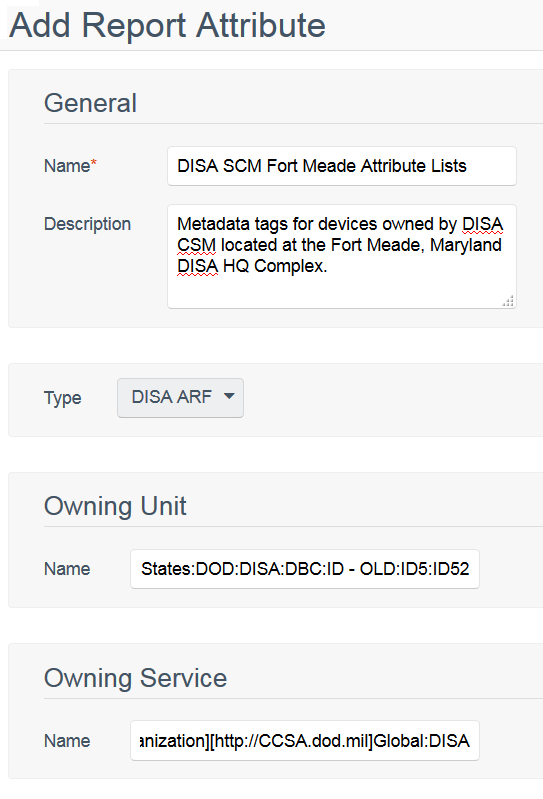
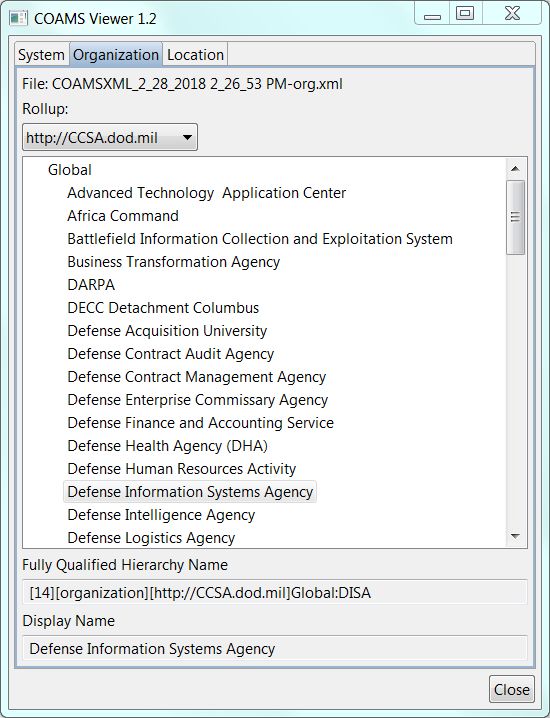
Within SecurityCenter, the user will need to add the following information:

* Create a descriptive name for the report attributes group  
  - Describe the group so as to allow for full understanding of its scope and intent
* Select Type as “DISA ARF”

Select the appropriate “Owning Organization” from COAMS Viewer. Paste the resulting text from COAMS Viewer’s “Fully Qualified Hierarchy Name” field into the “Owning Unit Name” field of SecurityCenter.

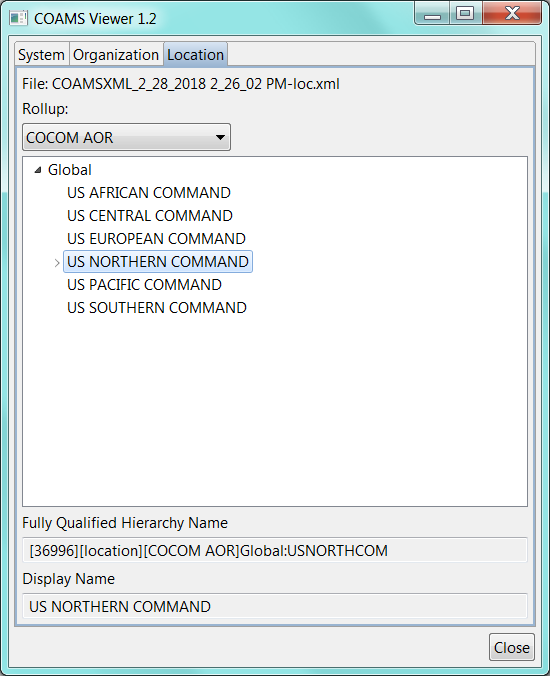
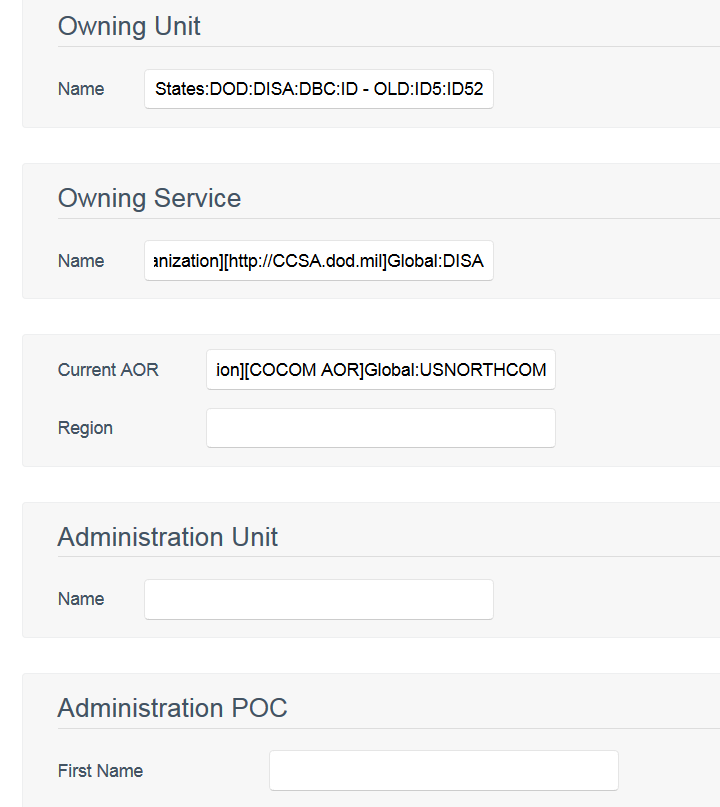
|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Note that the COAMS Viewer information follows what is needed to support the SecurityCenter fields. As the screen shots change in each step, the COAMS Viewer location changes |

***Step 2***



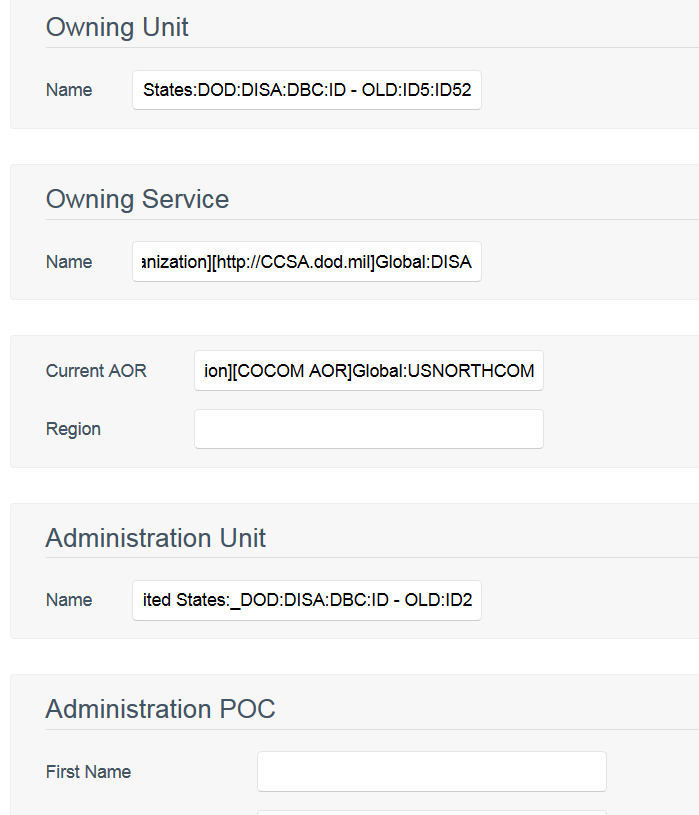
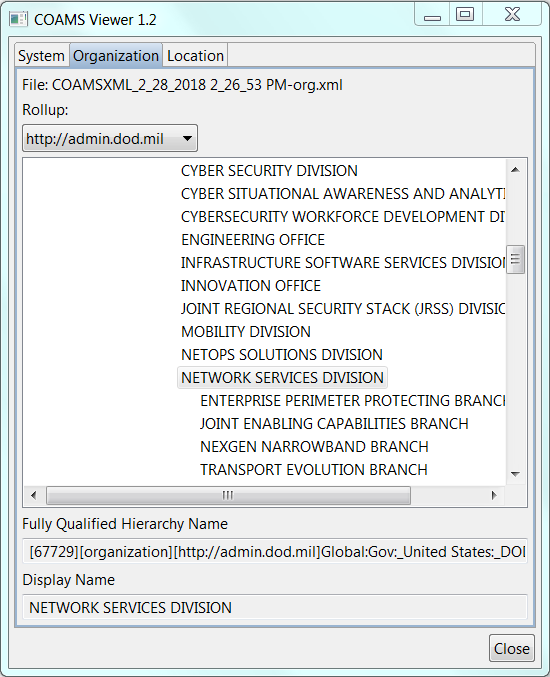
Select the appropriate “Owning CC/S/A” from COAMS Viewer’s Combatant Command/Service/Agency (CC/S/A) rollup in the “Organization” tab. Paste the resulting text from COAMS Viewer’s “Fully Qualified Hierarchy Name” field into the “Owning Service Name” field of SecurityCenter.

***Step 3***

******

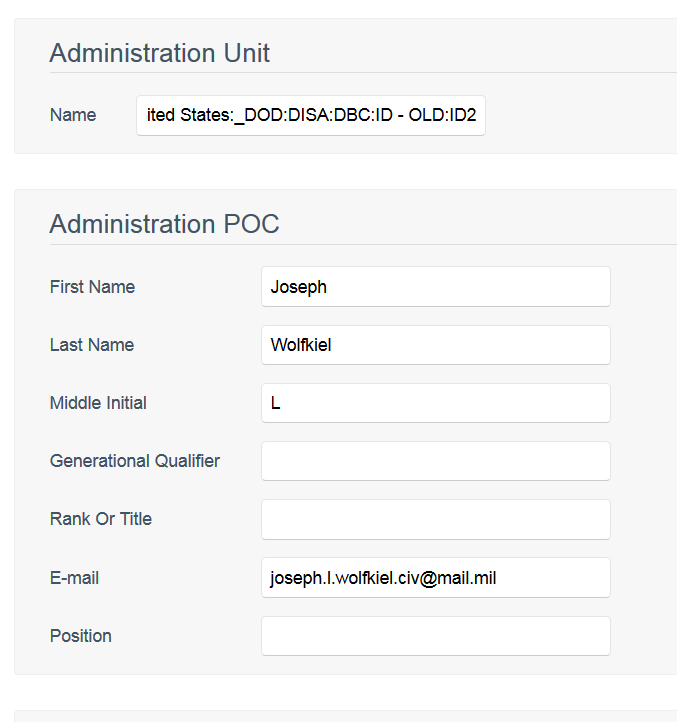
Select the appropriate “COCOM AOR” from COAMS Viewer’s COCOM AOR rollup in the “Location” tab. Paste the resulting text from COAMS Viewer’s “Fully Qualified Hierarchy Name” field into the “Current AOR” field of SecurityCenter. The “region” field of SecurityCenter is an optional field.

***Step 4***



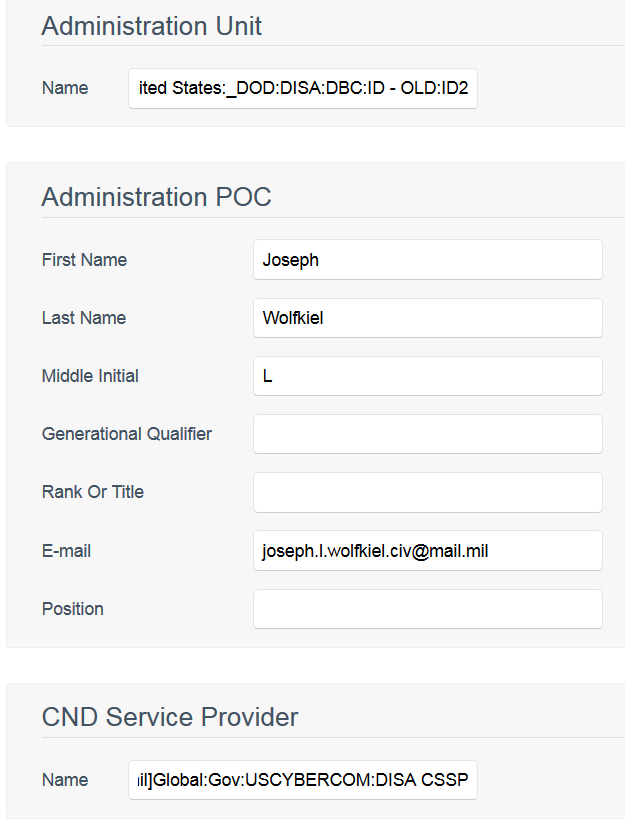
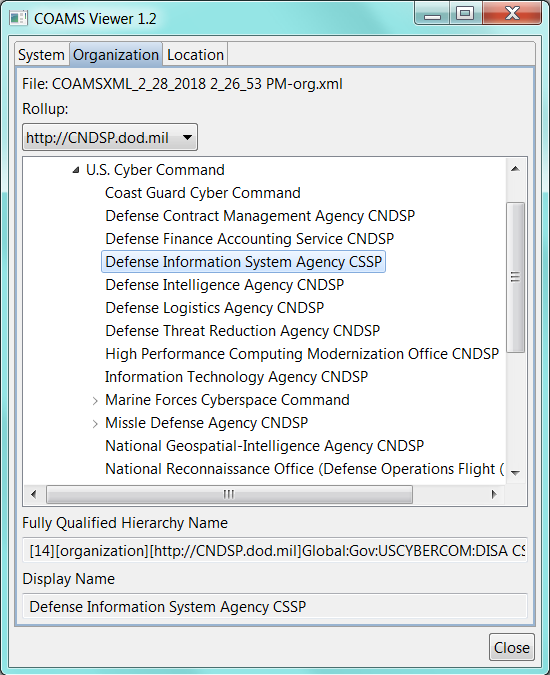
Select the appropriate “administering organization” from COAMS Viewer’s admin rollup in the “Organization” tab. Paste the resulting text from COAMS Viewer’s “Fully Qualified Hierarchy Name” field into the “Administration Unit Name” field of SecurityCenter.

***Step 5***

******

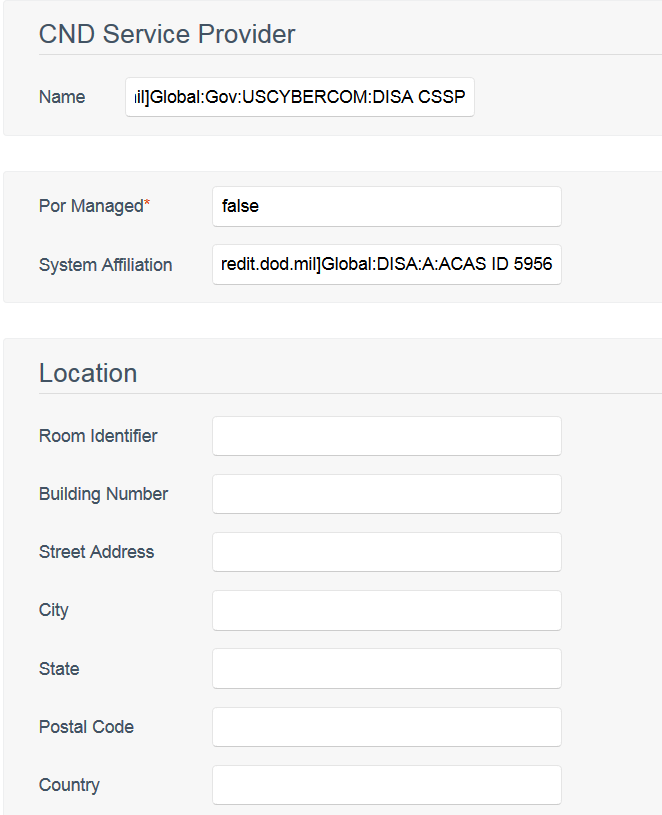
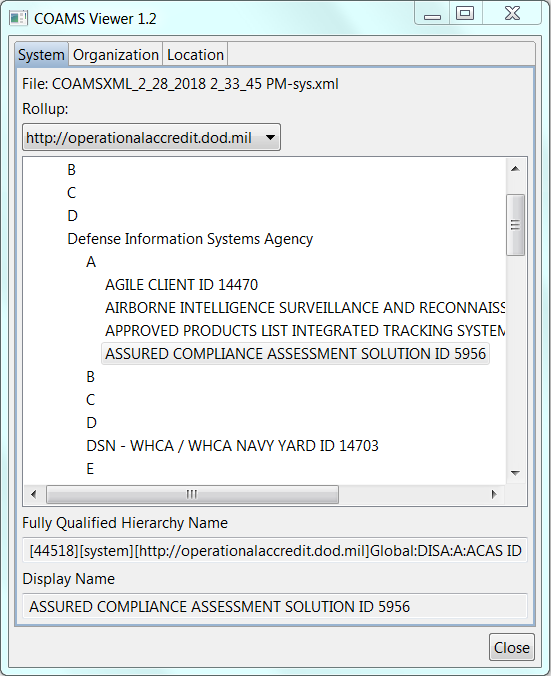
Type in any required information about an Administration Unit’s Point of Contact (POC) in SecurityCenter. Do not use the “generational qualifier” field of SecurityCenter.

***Step 6***



Select the appropriate “Computer Network Defense Service Provider” from COAMS Viewer’s Computer Network Defense Service Provider (CNDSP) rollup in the “Organization” tab. Paste the resulting text from COAMS Viewer’s “Fully Qualified Hierarchy Name” field into the “CND Service Provider Name” field of SecurityCenter.

***Step 7***



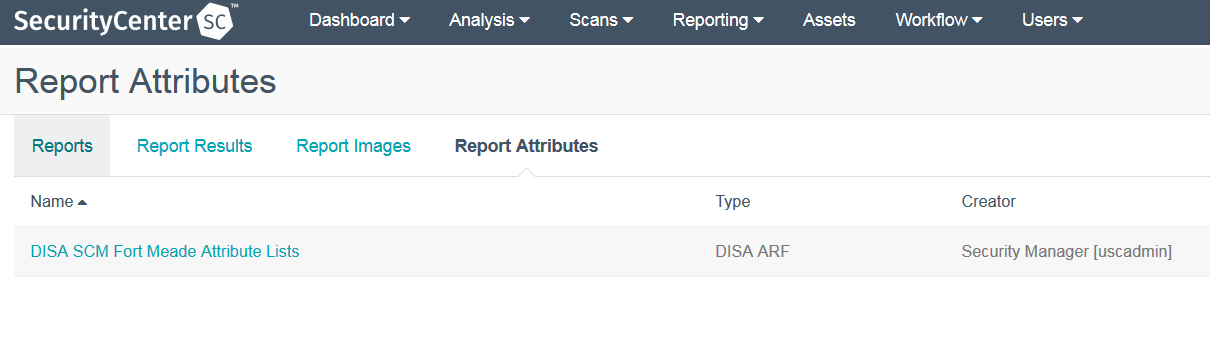
Set the “Por Managed” field of SecurityCenter to either “true” or “false” based on whether the assets being reported are centrally configuration managed by a Program Management Office (true) or not (false).

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | The values “true” or “false” must be in all lowercase. |

Select the appropriate “system affiliation name” from COAMS Viewer’s “operationalacredit” rollup in the “System” tab. Paste the resulting text from COAMS Viewer’s “Fully Qualified Hierarchy Name” field into the “System Affiliation” field of SecurityCenter.

Select the appropriate “location area” from COAMS Viewer’s “geolocation” rollup in the “Location” tab. Paste the resulting text from COAMS Viewer’s “Fully Qualified Hierarchy Name” field into the “Street Address” field under the “Location” section of SecurityCenter.

***Step 8***

******

Select the “Save” button to save the set of operational attributes in SecurityCenter.

# Using CMRS in SecurityCenter

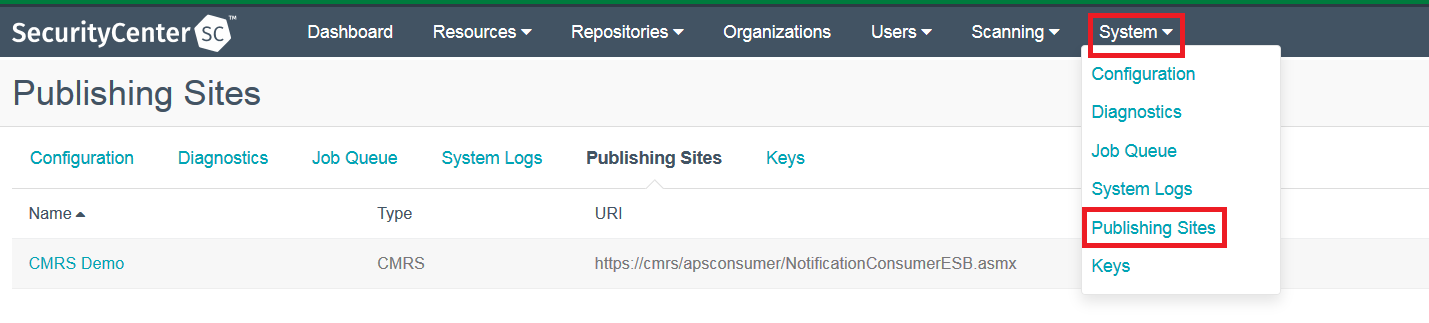
SecurityCenter has a feature which allows the ACAS data that is collected during a scan to be forwarded to CMRS. SecurityCenter will be able to generate two specific reports:

* *Assessment Summary Results* (*ASR*)
* *Assessment Results Format* (*ARF*).

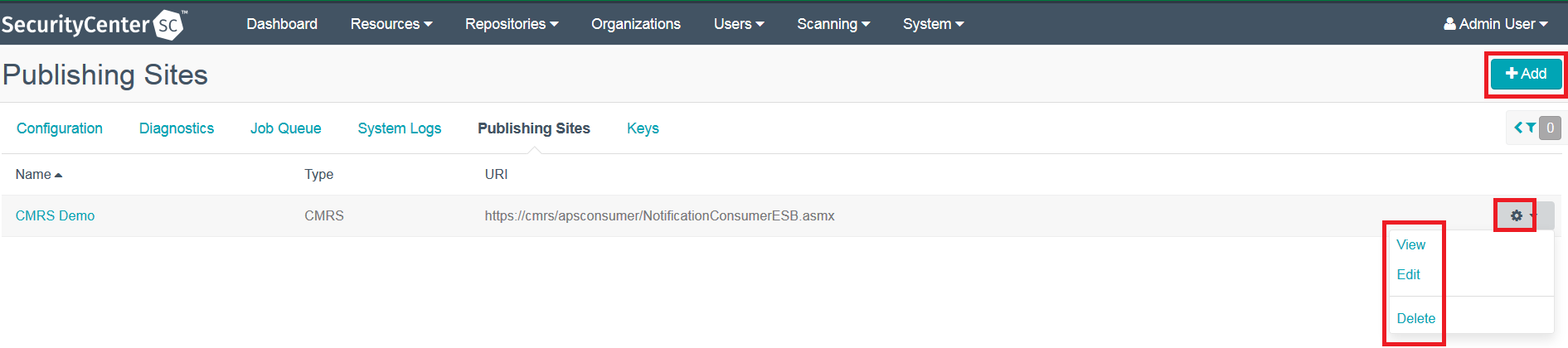
These report types are basic files in an **.xml** format that tags the information that is needed for CMRS. There is an option for publishing to other locations as long as it can accept the XML data tags. The files can be automatically sent out or manually reviewed. If reviewing locally the user must use an XML viewer.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | If the publishing site is using a self-signed certificate, in order to successfully test the publishing you may have to turn on debugging for publishing to relax the SSL CERT options for CURL and enable successful HTTPS communication with the CMRS server (the alternative to this is to install the appropriate CA for use by SecurityCenter, much like is done with setting up CAC card users). To turn on the debugging and relax the SSL CERT options, logon to the console of the SecurityCenter box and perform the following command:  # touch /opt/sc/admin/debug.publishing |

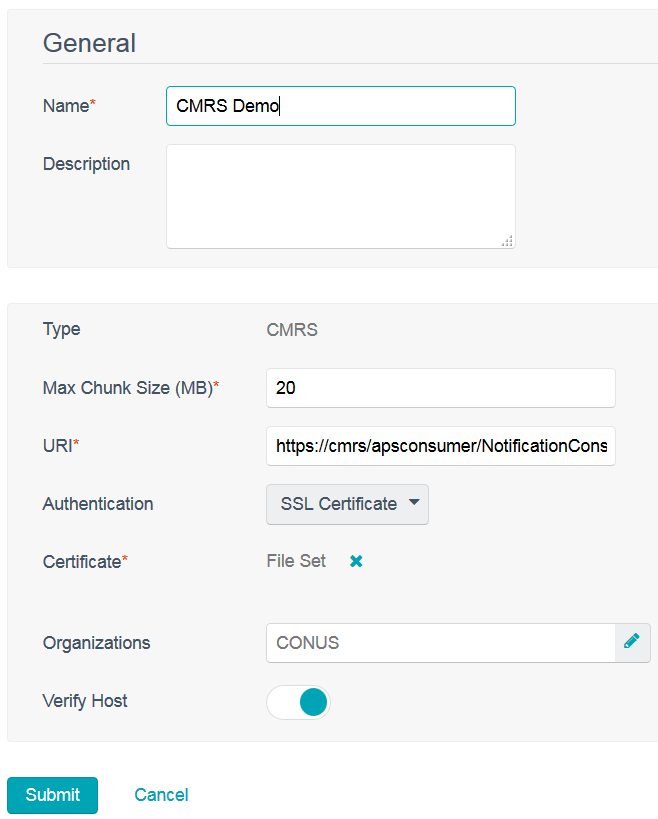
Now that an appropriate report attribute has been created for asset tagging a CMRS Publishing Site must be created for SecurityCenter to publish data to CMRS. Access to Publishing Sites is limited to only accounts with an Admin role. Publishing Sites can be access by clicking on “System” at the right-hand corner of the SecurityCenter navigation bar and clicking on “Publishing Sites”.



Selecting this menu option takes the user to the “Publishing Sites” page view, with Add, Edit, view Details, and Delete options, as well as a list of existing Publishing sites.



Clicking the Add button brings up the following “Add Publishing Site” dialog:

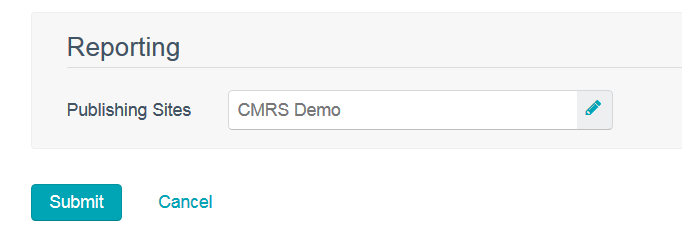


* **Name** is how the Publishing Site will be identified for selection.
* **Description** is a text block for the purpose it implies.
* **Type** is the type of communication used for the Publishing Site, which will be either HTTP POST or CMRS. Selecting “CMRS” changes the form view to display a **Max Chunk Size (MB)** field, which is the size pieces or “chunks” that the report being published will be broken up into for transmission. The default value is set to “20”. A value of “0” will disable the chunking of data feature.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | ACAS users are directed to use the default chunk size of 20MB. |

* **URI** contains the URI of the Publishing.
* **Authentication** is a drop-down for how SecurityCenter will identify itself/login to the Publishing Site. Currently, the choices are Password and Server Cert. Choosing Password changes the form view to display a **Username** and **Password** field for the credentials to be used. Server Cert has an accompanying **Certificate** field with a Browse button for uploading a certificate to use with the Publishing Site.
* **Organizations** displays the Organizations that are allowed to use the Publishing Site that is being configured. You can also add to an Organization’s list of available Publishing Sites when adding/editing an Organization.

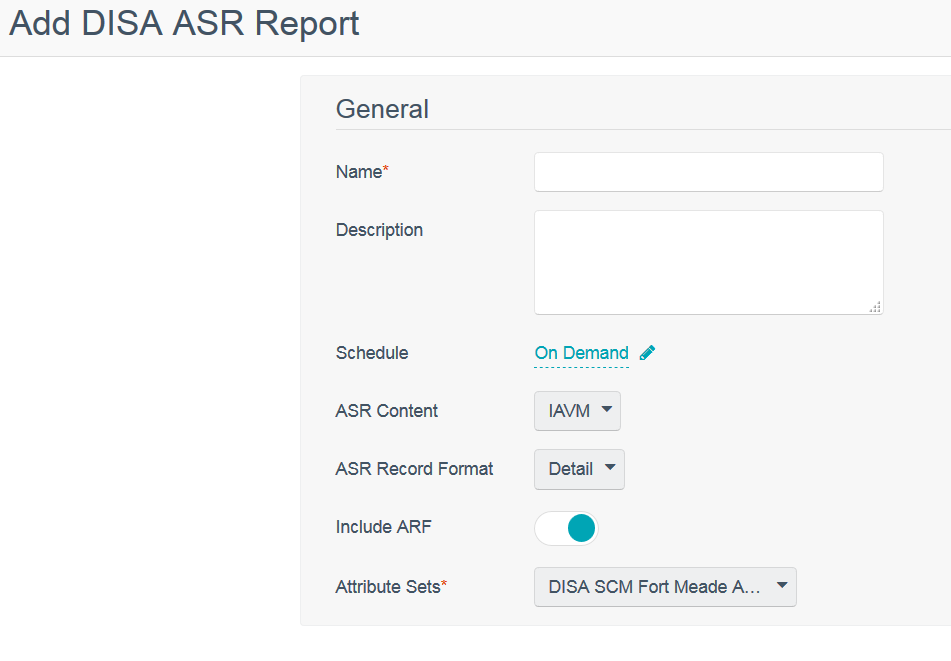
Once the Publishing Site has been created an Admin role user will need to enable the new Publishing Site for Organizational users. As an Admin click “Organizations” from the navigation bar. Select the Organization publishing to CMRS, scroll down to the “Reporting” section and select the Publishing Site created in the previous set. The screen should look similar to the example below. To save the new Organization configuration click “Submit”.



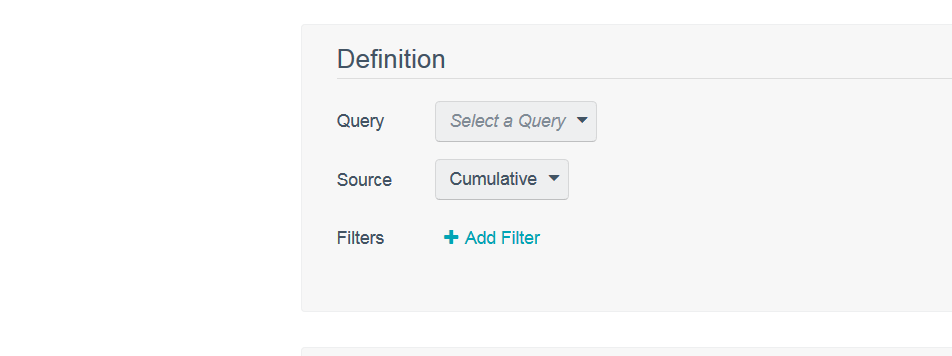
To actually publish to a Publishing Site, an Organizational user (in an Organization that has a Publishing Site defined and assigned to it) would create a report of “Type” DISA ARF, DISA ASR, or CyberScope.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Other “Type” selections may show the Publishing Site selection on the Distribution tab, but nothing will be published for those types. |

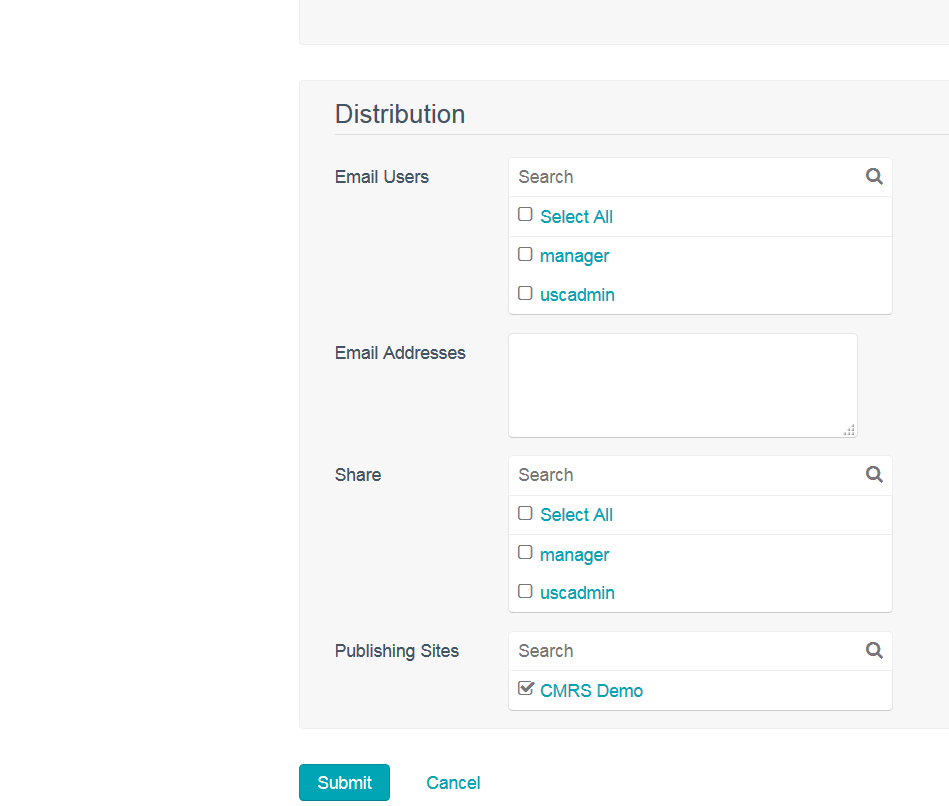
For publishing to CMRS add a new ASR type report. In the General tab be sure to select either IAVM, CVE, Plugin, or Benchmark as the ASR Content. The ASR Record Format must be “Detail”. Enable “Include ARF” and select the report attribute set created in *Using COAMS Viewer in SecurityCenter*.



In the ASR report’s Definition tab a pre-defined query and be used for filtering. The report’s data source can be either Cumulative (SC repositories) or Individual Scan result. Custom filters can be created to further filter the data to be used in the ASR report.



On the Distribution tab, select the Publishing Sites that the reports will be sent to at the end of running a report. Click “Submit” to save the new ASR report.

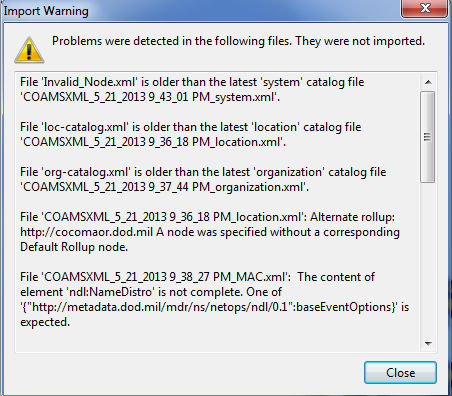


This report can be launched from the report screen. It can also be automatically run as a post-scan option from the “Post Scan” tab in a scan. When the report completes it will publish to the Publishing Site(s) selected as long as the receiving system is setup as a web service.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Multiple Publishing Sites, Report Attributes, and reports can be used by an Organization to accomplish publishing and asset tagging requirements. |

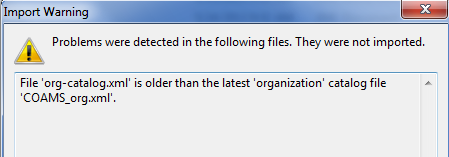
# Common Errors

When loading the COAMS Viewer, the system will validate the XML files to ensure they are compliant to the schema. Below is a collection of invalid XML errors, explanations, and resolutions to the errors. The errors will be listed in a pop up prior to the COAMS Viewer being loaded.



**Figure 2 – Sample Error Pop-up**

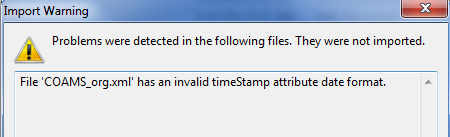
## Superseding Error



**Figure 3 – Superseding Error**

There is no resolution for this error. The COAMS Viewer detects two files of the same data type and indicates which file is the most current. The superseded file will not be loaded.

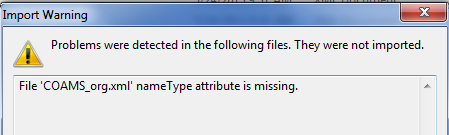
## Invalid Timestamp Error



**Figure 4 – Invalid Timestamp Error**

Download a valid COAMS catalog file and verify that the timeStamp is valid. Example: 2012-03-28T20:51:09.697Z (year-mo-dayThr:min:sec.milisecondZ).

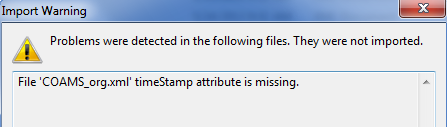
## Data Type Identifier Error



**Figure 5 – nameType Error**

The file must contain the nameType attribute to identify what data type is contained (Organization, Location etc.). Download a valid COAMS catalog file.

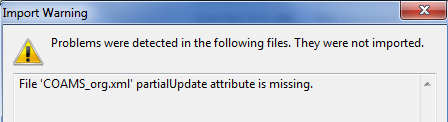
## Timestamp Missing Error



**Figure 6 - Timestamp Error**

The timestamp attribute is required in the header. Download a valid COAMS catalog file.

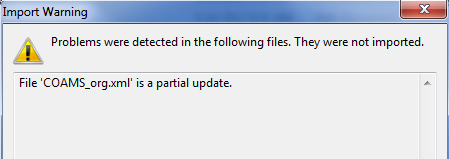
## Partial Update Error



**Figure 7 – Partial Update Error**

The partialUpdate attribute must be included in the header of the file. Download a valid COAMS catalog file.

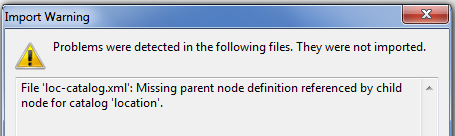
## Partial Update Value Error



**Figure 8 – Partial Update Value Error**

The XML file is flagged as a partial update which is not supported. Only full catalogs are supported. Verify that the latest catalog is being used.

## Missing Parent Error



**Figure 9 – Missing Parent Error**

The XML is identifying a node to a parent that has not been created. Download a valid COAMS catalog file.

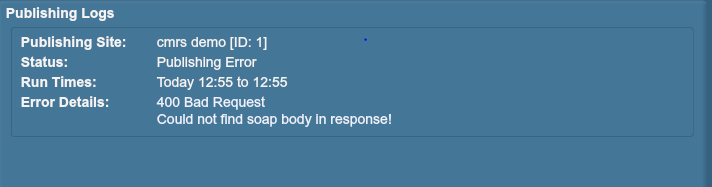
## Publishing Error

The issue comes when COAMs information is copied and pasted into the operational attributes in SecurityCenter.

Particular Publishing error:

400 Bad Request

Could not find soap body in response!



**Figure 10 – Publishing Report Error**

CMRS will not accept the following characters when publishing from SecurityCenter: “&”, “>”, or “<”. If the data makes it all the way to CMRS, CMRS only looks for an integer in between two brackets (e.g. [2005]). It doesn't read the text. As a work around, the user can just delete the signs and everything should work fine.

# Useful links

***Certification and Accreditation Artifacts***

Posted at ACAS SIPR Wiki: <http://www.intelink.sgov.gov/wiki/ACAS>

***ACAS Best Practices Guide***

Posted at: <https://patches.csd.disa.mil/Metadata.aspx?id=103248>

***ACAS Wiki***

<https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/Home.aspx>

***Approved documentation/binaries are located on DoD Patch Repository***

Posted at: <https://patches.csd.disa.mil/CollectionInfo.aspx?id=442>

(CAC is required for access). Click on ACAS > ACAS Software > then whichever application you need.

***ACAS License Portal***

<https://deps.disa.mil/ext/cop/mae/netops/acas/SitePages/requestPortal/LicenseRequest.aspx>

***Plugin Updates (Automatic Updates)***

Files are posted at <https://acas-update.csd/disa.mil>

***Plugin Updates (Manual Updates)***

<https://patches.mont.disa.mil/CollectionInfo.aspx?id=552>

***Software Forge***

All of our test and development efforts are located here and do not represent the approved baselines. <https://software.forge.mil/sf/frs/do/listReleases/projects.acas/frs.kickstart_image>

***Cyber Defense Training Cloud (CDTC)***

<https://cdtc.cert.org/lms>

***ACAS Customer Support/OKC Helpdesk***  
- NIPR: [disa.tinker.eis.mbx.okc-disa-peo-service-desk@mail.mil](mailto:disa.tinker.eis.mbx.okc-disa-peo-service-desk@mail.mil)

- SIPR: [disa.tinker.esd.mbx.okc-service-desk@mail.smil.mil](mailto:disa.tinker.esd.mbx.okc-service-desk@mail.smil.mil)

- DSN: 850-0032   
- COMM: 844-347-2457, opt 1, then 5